



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 150  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/625,363

07/23/2003

Ramarathnam Venkatesan

MS1-1285US

8229

22801

7590

03/16/2007

LEE & HAYES PLLC

421 W RIVERSIDE AVENUE SUITE 500

SPOKANE, WA 99201

EXAMINER

GEE, JASON KAI YIN

ART UNIT

PAPER NUMBER

2134

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
--	-------------------	---------------

3 MONTHS

03/16/2007

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/16/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@lechayes.com

<b>Office Action Summary</b>	Application No. 10/625,363	Applicant(s) VENKATESAN ET AL.	
	Examiner Jason K. Gee	Art Unit 2134	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

**A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.**

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 January 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-20 and 26-38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 and 26-38 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 July 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>07/23/2003</u> . | 6) <input type="checkbox"/> Other: _____  |

***DETAILED ACTION***

1. This action is response to communication: response to restriction filed on 01/12/2007 with acknowledgement of original filing date of 07/23/2003.
2. Claims 1-20 and 26-38 are currently pending in this application. Claims 21-25 and 39-43 have been withdrawn. Claims 1, 11, 12, 20, 26, 28, 29, 37, and 38 are independent claims.
3. The IDS received 08/11/2005 has been accepted.

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-20 and 26-38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 1-11, the independent claims recite "generating one or more codes". It is unclear what encompasses the generation of code, and what exactly the code that created is. Also, it is unclear what the metes and bounds are for the limitation of "reporting the one or more codes." If claim 1 is directed to creating within a system code and the reporting the code is making it available to the system, there is no tangible result and a 101 issue would arise.

As per claims 2-11, the claims recite "a medium as recited...". It is unclear whether this medium is the recited said medium in the claims in which they are dependent on.

As per claims 5, 6, 15, 16, 31 and 32, the claims recite the "length" of messages and codes. It is unclear what the "length" of the messages and codes are, as it could be bit length, size length, etc.

As per claim 8, the claims recite a "non-linear mathematical function, namely a quadratic equation." It is unclear what the metes and bounds of the claims are, and if the non-linear mathematical function has to be a quadratic equation, or could it be another non-linear mathematical function.

As per claim 10 and 36, the claims recite "the reported codes r and s". There is insufficient antecedent basis for these limitations, and it is unclear what encompasses "r" and "s".

As per claims 11 and 20, the claims recite audio/visual output. It is unclear whether this limits it to "audio and visual" output, or "audio or visual" output.

As per claims 12-20 and 26-38, the independent claims recite "generating one or more codes". It is unclear what encompasses the generation of code, and what exactly the code that created is. Also, it is unclear what the metes and bounds are for the limitation of "reporting the one or more codes." If the independent claim is directed to creating within a system code and the reporting the code is making it available to the system, there is no tangible result and a 101 issue would arise. Furthermore, as per claims 12-20, the claims recite  $g^k$ . It is unclear what  $g^k$  encompasses.

Art Unit: 2134

As per claims 13-25, the claims recite "a medium as recited...". It is unclear whether this medium is the recited said medium in the claims in which they are dependent on.

As there are many 112 issues regarding clarity of the claims, the claims will be rejected as best understood by the Examiner.

***Claim Rejections - 35 USC § 101***

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 37 and 38 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As per claims 37 and 38, the claims recite a message embodied on a computer readable medium and a message on a human-readable medium. A produced message embodied on a medium is directed to non-statutory subject matter.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-4, 7-14, 17-20, 26-28, 30, 33, 34, 36, and 37 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Pointsov European Patent Application EP 1083700 A2 (03/14/2001)..

As per claim 1, Pintsove teaches a computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising: obtaining a message M having two portions, wherein M1 is one of the portions of the M and M2 is another (paragraph 8, wherein M2 is the hidden first portion, and M1 is the visible second portion); generating one or more codes having a combination with M2 implicitly embedded therein, wherein calculations that generate the one or more codes do not employ M2 (paragraph 8, wherein code is created by encrypting the hidden first portion; also, code is created by combining an encrypted M1 with M2 and hashing them together); reporting the one or more codes (paragraph 8, wherein the code is reported to be used for creating a second portion and also for creating a signature).

As per claim 2, Pintsove teaches wherein the method further comprises producing a digital signature (DS) comprising M1 and the reported one or more codes (paragraph 8, wherein a signature comprises the first and second components with the visible portion (M1) ).

As per claim 3, Pintsove teaches wherein two or more codes are generated by the generated and reported by the reporting (paragraph 8, wherein one code is the first component, and the second code is the second component).

As per claim 4, Pintsove teaches wherein a mathematical function for calculating one code is not identical to a mathematical function for calculating another code (paragraph 8, 20, 21; Figure 1).

As per claim 7, Pintsove teaches wherein the generating comprises: finding a value of a variable per-message key ( $k$ ) where a predefined mathematical function employing  $k$  produces a result equivalent to M2 (paragraphs 19-25, and 29); when such a value of  $k$  is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates  $k$  (paragraphs 19-25, and 29).

Claim 8 is rejected using the same basis of arguments used to reject claim 7. Non-linear mathematical functions are taught throughout Pintsove, such as in paragraphs 14 and 29, wherein DES and SHA both employ non-linear mathematical functions.

As per claim 9, as best understood by the Examiner, Pintsove teaches finding a value of a variable per-message key ( $k$ ) where a predefined mathematical function

Art Unit: 2134

employing  $M1$  and  $g^k$  produces a result equivalent to  $M2$  (paragraphs 19-25, and 29); when such a value of  $k$  is found, calculating the two or more codes, where one code is  $r$  (paragraphs 19-25, and 29, where  $r$  is  $c$ ) and another is  $s$  (paragraphs 19-25, and 29, where  $s$  is  $s$ ), with  $r$  ( $c$ ) being calculated using another predefined mathematical function employing  $M1$  and  $g^k$  (paragraphs 19-25, and 29), and with  $s$  being calculated using still another predefined mathematical function employing  $M1$ , and  $g^k$  and  $r$  (paragraphs 19-25, and 29, wherein  $s = k^{-1} \{ \text{SHA1}(c/V) + ar \} \bmod n$ ).

As per claim 10, Pintsove teaches wherein the method further comprises producing a digital signature (DS) comprising  $M1$  and the reported codes  $r$  and  $s$  (paragraphs 8 and 29, wherein the signature is  $(s, c, V)$ ).

Independent claim 11 is rejected using the same basis of arguments used to reject claim 1. Video output is taught throughout the reference, as a portion of the message is a visible portion. A portion is not visible unless it may be displayed on an output.

Independent claim 12 is rejected using the same basis of arguments used to reject claims 8 and 9.

Claim 13 is rejected using the same basis of arguments used to reject claim 10.

Claim 14 is rejected using the same basis of arguments used to reject claim 8.

Claim 17 is rejected using the same basis of arguments used to reject claim 9 above.

Claim 18 is rejected using the same basis of arguments used to reject claim 8 above.



Claim 19 is rejected using the same basis of arguments used to reject claim 10 above.

Independent claim 20 is rejected using the same basis of arguments used to reject claim 11 above.

Independent claim 26 is rejected using the same basis of arguments used to reject claim 12 above.

Claim 27 is rejected using the same basis of arguments used to reject claim 13 above.

As per claim 28, Pointsov teaches a digital signature created throughout the reference. As the digital signature is created on a computer, as taught throughout the reference, it would be inherent that the digital signature is stored on a computer-readable medium, at least temporarily. The other limitations of the claims are rejected using the same basis of arguments used to reject claim 27.

Claim 30 is rejected using the same basis of arguments used to reject claim 14 above.

Claim 33 is rejected using the same basis of arguments used to reject claim 17 above.

Claim 34 is rejected using the same basis of arguments used to reject claim 18 above.

Claim 36 is rejected using the same basis of arguments used to reject claim 19, wherein a message is a digital signature.

Claim 37 is rejected using the same basis of arguments used to reject claim 28 and 36 above, wherein a digital signature is a type of message.

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 5, 6, 15, 16, 29, 31, 32, 35, and 38 are rejected under 35 U.S.C. 103(a) as being obvious over Pintsov European Patent Application Ep 1083700 A2 (hereinafter Pintsov).

As per claim 5, as best understood by the Examiner, Pintsov teaches wherein the message M has a defined length (paragraph 9, wherein M1 and M2 (the combination of M1 and M2 make up M) have a determined length). However, at the time of the invention, Pintsov does not explicitly teach wherein the length of the combination of the two or more codes is less than the message's defined length. Pintsov teaches though that the two codes are hashed though in paragraph 8 and throughout the reference. It is well known in the art that hashing reduces the data into a small number that serves

Art Unit: 2134

as a fingerprint. If both the codes were hashed to less than half the size, it would be true that the length of a combination of two or more codes is less than the message's defined length.

At the time of the invention, it would have been obvious to have the length of a combination of two or more codes to be less than the message's defined length. One of ordinary skill in the art would have been motivated to perform such an addition to increase the speed of the whole process and a better flow of data by having codes that are smaller than half the size of the original message.

Claim 15 is rejected using the same basis of arguments used to reject claim 5 above.

Claim 31 is rejected using the same basis of arguments used to reject claim 5 above.

As per claim 6, as best understood by the Examiner, Pintsov teaches wherein M2 has a defined length (paragraph 9, wherein M2, the first portion, has a size determined by an application). However, at the time of the invention, Pintsov does not explicitly teach wherein the length of the combination of the two or more codes is less than the defined length of M2. Pintsov teaches though that the two codes are hashed in paragraph 8 and throughout the reference. It is well known in the art that hashing reduces the data into a small number that serves as a fingerprint. If both the codes were hashed to less than half the size, it would be true that the length of a combination of two or more codes is less than M2's defined length.

At the time of the invention, it would have been obvious to have the length of a combination of two or more codes to be less than M2's defined length. One of ordinary skill in the art would have been motivated to perform such an addition to increase the speed of the whole process and a better flow of data by having codes that are smaller than half the size of the original message.

Claim 16 is rejected using the same basis of arguments used to reject claim 6 above.

Claim 32 is rejected using the same basis of arguments used to reject claim 6 above.

As per claim 29, Pointsov does not explicitly teach wherein a digital signature is embodied as human-readable indicia on a human readable medium. However, a digital signature embodied as human-readable indicia on a human-readable medium is well known in the art and it would have been obvious to do so. One of ordinary skill in the art would have been motivated to perform such an addition as to be able to provide a digital signature so that humans can be able to see it and confirm the signature visually. Also, providing a signature that can be confirmed visually would be practical and would require less calculations. The remaining limitations of the claims are rejected using the same basis of arguments used to reject claim 27 above.

Claim 38 is rejected using the same basis of arguments used to reject claim 29 and 36 above, wherein a digital signature is a type of a message.

As per claim 35, Pointsov teaches all the limitations of the claims, but does not explicitly teach wherein the predefined mathematical function for  $s$  is quadratic. As can be seen in the rejection for claim 34, Pointsov teaches that the predefined mathematical function for  $s$  is non-linear. However, a quadratic equation is well known in the art, and would be obvious to implement. At the time of the invention, it would have been obvious to one of ordinary skill in the art to include a quadratic as the mathematical function for  $s$ . Quadratics are well known in the art, and easy to solve, and it would have been obvious to include a quadratic equation as a non-linear equation.

### ***Conclusion***


11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee  
Patent Examiner  
Technology Center 2134  
03/08/2007

  
KAMBIZ ZAND  
PRIMARY EXAMINER